

# CRIMES VIRTUAIS

Camila Queiroga Gentil<sup>1</sup>  
Maria Luiza Figueiredo Heine<sup>2</sup>  
Ilzver Matos<sup>3</sup>

Direito



## RESUMO

O presente artigo visa ampliar o conhecimento sobre os crimes virtuais. Trata-se de crimes virtuais os crimes cometidos na internet, por meio de e-mails, mensagens, vídeos, fotos ou qualquer outro meio de comunicação nas redes eletrônicas. Em sua maioria, crimes que atingem a honra e moral da vítima. E apresenta um breve resumo sobre a lei 12.737/12, única legislação disponível para combate de tais delitos.

## PALAVRAS-CHAVE

Internet; Lei 12.737/12; Crimes virtuais; Vazamento de dados.

## ABSTRACT

This article aims to increase knowledge about virtual crimes. These are virtual crimes of crimes committed on the Internet, through emails, messages, videos, photos or other means of communication in electronic networks. Mostly crimes that strike the honor and morale of the victim. And it presents a brief summary on a law number 12.737 / 12, a single legislation available for the combat of such crimes.

## KEYWORDS

Internet. Law 12,737 / 12. Virtual Crimes. Leakage of Data.

## 1 INTRODUÇÃO

Durante a Guerra fria, os militares norte-americanos criaram um meio para manter comunicação em caso de ataques inimigos que destruíssem os outros meios de comunicação, assim surgia a internet.

Os primeiros registros de crimes cibernéticos vieram aparecer em meados da década de 1970, onde originariamente foi criado o termo “*hacker*” – que nada mais é do que um indivíduo conhecedor de sistemas técnicos que utiliza a rede de informações para roubar dados em gerais. A partir de 1980 quando a internet começa a ser comercializada para uso pessoal, pode-se notar o engajamento criminoso no campo virtual, que com o passar das décadas esse problema foi ganhando uma maior dimensão, conforme a maior acessibilidade a esse meio de propagação.

O acesso às diversas informações que ficam disponíveis na imensidão do campo virtual desperta interesse nos criminosos, visto que podem utilizar desse meio virtual para obter vantagens ilícitas. Diz Ivette Ferreira (2002 apud CRISPIN, 2011, p. 25):

A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução.

Segundo informações da multinacional Symantec, empresa de segurança na internet, em 2012: 60% dos brasileiros foram vítimas do cybercrime, um total de 22 milhões de pessoas; 45% dos adultos no país tiveram uma experiência de crime vir-

tual e comportamento de risco nos últimos 12 meses do ano; 39% dos usuários de smartphone no Brasil afirmam que não deletam e-mails suspeitos de pessoas que não conhecem (SYMANTEC, 2016, on-line).

## 2 FUNDAMENTAÇÃO TEÓRICA

Segundo Ramalho Terceiro (2006, não paginado), os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo; por isso, ficaram usualmente definidos como sendo crimes virtuais. Ou seja, os delitos praticados por meio da Internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.

Já de acordo com Augusto Rossini (2004 apud SENNA, 2014, on-line), o conceito de delito informático poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

A denominação “delitos informáticos”, segundo Rossini (2004 apud SENNA, 2014, on-line), abarca crimes e contravenções penais, alcançando não somente aquelas condutas praticadas no âmbito virtual, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível conexão na Rede Mundial de Computadores, ou a qualquer outro ambiente telemático.

Ou seja, uma fraude em que o computador é usado como instrumento do crime, fora da Internet, também seria alcançada pelo que se denominou delitos informáticos. Ainda para o autor, “delito informático” é gênero, do qual “delito telemático” é espécie, dada a peculiaridade de ocorrer no inter-relacionamento entre os computadores em rede telemática usados na prática delitiva.

Segundo Guimarães e Furlaneto Neto (2003, on-line), crime virtual será qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados. Tais crimes, por não estarem devidamente tipificados no âmbito penal, não são passíveis de punição, ou seja, por não haver uma lei específica para tal, eles são tratados com analogia jurídica, como exemplo punir ofensas em redes sociais com os crimes contra a honra. Atualmente, não há legislação específica definindo o que é crime na rede. Assim, eventuais condenações são feitas com base no Código Penal, que foi reformado em 1984 – antes, portanto, da existência da Internet.

## 3 CLASSIFICAÇÃO DO CYBERCRIME

Os criminosos agem nesse meio por se sentirem seguros, achando que por estar na internet, não serão penalizados, o que não é verdade. Em sua grande maioria, temos uma extensa lista de crimes cometidos nesse âmbito, a exemplo de: roubo de identidades, apologia ou indução ao crime, pedofilia, ameaça etc.

O crime pode ser realizado por acesso direto ao computador ou à distância, por meio de *malware* criados para esse tipo de crime, por isso subdividem-se os crimes virtuais em puros ou impuros.

Os crimes puros serão aqueles em que o sujeito se utiliza do computador, onde este se torna objeto e meio do crime, alterando ou divulgando material próprio, atingindo diretamente o software ou hardware e que não tem sua conduta tipificada, precisando que a lei crie tipos penais específicos.

Crimes eletrônicos puros [...] são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. (JESUS, 2003 apud CARNEIRO, 2012, on-line).

Enquanto que nos crimes impuros – também chamados de mistos – é quando o agente utiliza do computador para meio ilícito, com isso tornando-o o meio para a execução do crime e possui tipificação para tal conduta realizada.

[...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não-computacionais ou diversos da informática. (JESUS, 2003 apud CARNEIRO, 2012, on-line).

## 4 AGENTES E FALTA DE LEGISLAÇÃO

Um dos principais problemas da identificação do criminoso é que não tem sua presença física no momento da conduta criminosa, no campo virtual ele pode estar em qualquer lugar do mundo. Para melhor entendimento existe a denominação de cada sujeito.

*Hacker*: são aqueles que invadem computadores, furtando dados e espalhando vírus;

*Cracker*: quem boicota programas de computadores, fornecendo senhas e chaves que foram obtidas de forma ilícita;

*Lammer*: os que não têm muito conhecimento de informática, não apresenta muito risco;

*Spammer*: indivíduos que invadem a privacidade de outrem por meios de mensagens eletrônicas.

Como anteriormente mencionado, a conduta criminosa é realizada no campo virtual, não existe a presença física do agente, isso dificulta a apreensão do criminoso.

Quanto à legislação aplicada nesses crimes, temos uma ineficiência por parte do nosso ordenamento jurídico, a falta de uma legislação específica para os crimes cibernéticos, necessitando de uma maior rigorosidade no combate desse crime. Além de uma legislação específica necessitamos que haja mais responsabilidade por parte dos usuários da internet quando da divulgação de dados pessoais. Hoje em dia o que mais notamos é o quanto estamos expostos nos meios sociais, por meio de redes de comunicações em massa. Muitos usuários não têm noção quanto está exposto e acaba divulgando suas intimidades para outrem, podendo-lhe gerar grandes problemas.

A desinformação e falta de prevenção ainda é muito grande. Por ser um espaço ainda novo, que dia após dia cresce, a população não enxerga o perigo constante ao qual está exposta, não entendendo que “caiu na rede, já era”. Uma vez on-line, não pode ser desfeito. A falta de leis específicas, que puna diretamente o autor e a facilidade em criar identidades falsas nesse meio, faz com que a punibilidade nesses crimes, se torne cada vez menor.

## **5 BREVE ANÁLISE SOBRE A LEI 12.737 – “LEI CAROLINA DIECKMANN”**

A única lei específica para o ambiente virtual na legislação brasileira é a Lei 12.737 que penaliza vazamento de dados, que surgiu, foi sancionada e publicada em 2012, tendo ficado bastante conhecida por seu apelido, que leva o nome da atriz Carolina Dieckmann, a qual teve seus dados pessoais divulgados na internet – inclusive fotos de caráter íntimo – após levar o seu computador em uma loja para reparo.

Esta lei acrescentou dispositivos legais que tipificam alguns delitos informáticos que sofriam com a insegurança constante no ambiente virtual. As invasões às redes e computadores, para obter dados e materiais pessoais, vinham causando grande prejuízo aos direitos individuais da população, portanto, com a criação de tal lei, há uma maneira de punir os agentes que antes tinham a segurança da internet para agir sem punição. Incluiu no Código Penal os artigos: 154-A, 154-B, 266 e 298.

### **5.1 ARTIGOS 154-A, 154-B, 266 E 298**

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Tem o objetivo de punir quem, por meio de computador ou internet, invade e torna público os dados pessoais de um usuário. Tem como pena 3 meses até 1 ano e multa. E mais, quem produz, vende ou distribui programa para tal, responde a mesma pena.

Ainda assegura punição para casos que tenha prejuízo econômico ou que seja obtido conteúdo sigiloso ou segredos comerciais. E se tal material seja vendido ou

transmitido a terceiros. O 154-B protege a administração pública da União, Estados, Municípios ou empresas terceirizadas dos mesmos, de tais crimes.

O artigo 266 trata da interrupção de serviços telefônicos ou informáticos, isto é, quem utiliza meios para derrubar o sinal e impede que as empresas restaurem. Por último, a falsificação de cartão de crédito ou débito, imposto no artigo 298 do nosso código penal.

Ao analisar tal tipo penal – invadir dispositivo informático – faz-se uma comparação com os elementos típicos de um crime doloso: conduta, resultado, causalidade, tipicidade, tentativa e consumação. Logo, vemos que tais crimes são sim de caráter penal.

Trata-se de crime condicionado a representação da vítima, logo muitos casos serão omitidos por falta de informação e de muitas acharem que não há penalização para estes crimes. Falta muito para o ambiente virtual ser seguro, mas a criação da lei em 2012 foi um avanço para a legislação brasileira.

## 6 CONSIDERAÇÕES FINAIS

A tecnologia avança sempre mais e com isso quem pratica os crimes virtuais são pessoas que veem na internet uma oportunidade de segurança e conforto para que possa fragilizar o outro, pessoas, em maioria, que agem com egoísmo, em busca de provocar e oprimir terceiros. Estes não percebem que a crescente busca por resolução de crimes virtuais está cada vez mais intensa, a justiça continua a lutar arduamente contra qualquer tipo de ato praticado no ambiente virtual.

Crimes como estes, por vezes tornam-se fatais, a vítima tem seus dados espalhados por uma rede mundial e a humilhação constante torna um ambiente propício de fraqueza da vítima que recorre ao suicídio como forma de aliviar. Nunca se sabe qual limite que foi alcançado uma vez que está na internet.

O Estado precisa manter-se atento, pois a sociedade evolui cada dia mais e os crimes acompanham o desenvolvimento. É preciso campanhas para orientação de pais e jovens sobre os crimes para ter o conhecimento devido.

Um mundo globalizado e interligado, precisa de lei para proteger num ambiente até hoje pouco conhecido, como é o virtual. A rede mundial de internet junto à liberdade e falsa segurança oferecida torna-se um local propício para crimes e, como tal, precisa de legislação viável para puni-los.

## REFERÊNCIAS

BARBOSA, Carina Luna Barbosa. **Crimes cibernéticos**: crimes de alta tecnologia. 2015. Disponível em: <<http://www.webartigos.com/artigos/crimes-ciberneticos-crimes-de-alta-tecnologia/129172/>>. Acesso em: 20 set. 2016.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico**, Rio Grande, XV, n.99, abr. 2012. Disponível em: <[http://www.ambito-juridico.com.br/site/?n\\_link=revista\\_](http://www.ambito-juridico.com.br/site/?n_link=revista_)

artigos\_leitura&artigo\_id=11529>. Acesso em: 10 jan. 2017.

CRISPIN, Mirian Cristina Generoso Ribeiro. Doutrina nacional: crimes praticados pela Internet e crimes de informática. ® **BuscaLegis.ccj.ufsc.br**, 2011. Disponível em: <<http://www.egov.ufsc.br/portal/conteudo/doutrina-nacional-crimes-praticados-pela-internet-e-crimes-de-inform%C3%A1tica>>. Acesso em: 5 dez. 2016.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. Crimes na internet: elementos para uma reflexão sobre a ética informacional. **R. CEJ**, Brasília, n.20, p.67-73, jan-mar. 2003. Disponível em: <<http://www.cjf.jus.br/revista/numero20/artigo9.pdf>> Acesso em: 10 nov. 2016

GRECO, Rogério. **Código penal comentado**. 5.ed. Niterói-RJ: Impetus, 2011.

GRECO, Rogério. **Curso de direito penal**: parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa. Niterói-RJ: Impetus, 2014.

JESUS, Damásio Evangelista de. **Direito penal**. 25.ed. São Paulo: Saraiva, 2014.  
MARCO CIVIL DA INTERNET: seus direitos e deveres em discussão. 2014. Disponível em: <<http://culturadigital.br/marcocivil/>>. Acesso em: 28 set. 2016.

MACHADO, Lucyana A. Crimes cibernéticos. **Direito Net**. 2014. Disponível em: <<http://www.direitonet.com.br/artigos/exibir/8772/Crimes-ciberneticos>>. Acesso em: 10 set. 2016.

NORONHA, Edgard Magalhães. **Direito penal**. Parte Geral. 24.ed. São Paulo: Saraiva, 1986.

OLIVEIRA, Luiz Gustavo Caratti de; DANI, Marília Gabriela Silva. Os crimes virtuais e a impunidade real. **Âmbito Jurídico**, Rio Grande, XIV, n.91, ago. 2011. Disponível em: <[http://www.ambito-juridico.com.br/site/index.php?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=9963](http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963)>. Acesso em: 10 out. 2016.

SALVADORI, Fausto. Crimes virtuais. **Galileu**, 2016. Disponível em: <<http://revistagalileu.globo.com/Revista/Common/0,,EMI110316-17778,00-CRIMES+VIRTUAIS.html>>. Acesso em: 10 jan. 2017.

SCHIMIDT, Guilherme. Crimes cibernéticos. **JusBrasil**. 2016. Disponível em: <<http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>>. Acesso em: 15 set. 2016.

SENNA, Tel. Crimes virtuais: uma análise jurídica no brasil. **Jus.com.br**. 2014. Disponível em: <<https://jus.com.br/artigos/32331/crimes-virtuais-uma-analise-juridica-no-brasil>>. Acesso em: 10 jan. 2017.

SILVEIRA, Artur Barbosa da. Os crimes cibernéticos e a lei nº 12.737/2012. **Conteúdo Jurídico**. 2015. Disponível em: <<http://www.conteudojuridico.com.br/artigo,os-crimes-ciberneticos-e-a-lei-no-127372012,52253.html>>. Acesso em: 23 set. 2016.

SYMANTEC. 2016. Disponível em: <[https://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20131002\\_01](https://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20131002_01)>. Acesso em: 20 maio 2016.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes virtuais**. 2005. Disponível em: <<http://www.advogadocriminalista.com.br>>. Acesso em: 20 maio 2016.

---

**Data do recebimento:** 23 de julho de 2017

**Data da avaliação:** 23 de novembro de 2017

**Data de aceite:** 12 de dezembro de 2017

---

---

1 Acadêmica do curso de Bacharelado em Direito da Universidade Tiradentes – UNIT. E-mail: camilaqueiroga@outlook.com.

2 Doutora em Educação e Contemporaneidade pela Universidade do Estado da Bahia – UNEB (2013); Mestra em Desenvolvimento Regional e Meio Ambiente pela Universidade Estadual de Santa Cruz – UESC (2004); Especialista em História Regional (1996); Graduada em Filosofia (1980); Professora credenciada da Universidade do Estado da Bahia no Mestrado Profissional Gestão e Tecnologia Aplicadas à Educação (GESTEC); Professora da Universidade Tiradentes – UNIT. E-mail: marialuizaheine3@gmail.com

3 Doutor em Direito pela Pontifícia Universidade Católica do Rio de Janeiro – PUC-RIO (2014); Mestre em Direito pela Universidade Federal da Bahia – UFBA (2008); Graduado em Direito pela Universidade Federal de Sergipe – UFS (2003); Foi bolsista do Programa Internacional de Bolsas de Pós-graduação da Fundação Ford – Internacional Fellowship Program – IFP; Realizou Mestrado-Sanduíche no Centro de Estudos Sociais- CES da Universidade de Coimbra; Professor da Universidade Tiradentes – UNIT. E-mail: ilzver@gmail.com